IN THE CLAIMS

What is claimed is:

1. A system for authenticating a subject residing in a subject domain on a network to a server application residing in a server domain on the network, wherein an authentication mechanism residing in an authentication domain on the network affects the service provided by the server application, the system comprising:

a client for communicating with other components of the system and for authenticating the subject to other components of the system by providing a client name assertion on behalf of the subject, wherein said client also resides in the subject domain; and

a protocol proxy for communicating between said client and the authentication mechanism and for authenticating said client based on said client name assertion, for obtaining from the authentication mechanism credentials for said client to access the server application, and for creating from said credentials an authentication name assertion allowing said client to access the server application.

2. The system of claim 1, wherein:

the subject is non-human and said client is integrated into the subject; and

said client gathers subject credentials for the subject and communicates said subject credentials to said protocol proxy.

3. The system of claim 1, wherein a plurality of the authentication mechanisms are present on the network, and the system further comprising:

an agent for communicating with other components of the system and for interacting with said client to chose an appropriate authentication mechanism from among said plurality of the authentication mechanisms, wherein said agent resides in an agent domain on the network.

4. The system of claim 3, wherein said client interacts with said protocol proxy to determine a specification of the authentication mechanism and said client communicates said specification to said agent.

5. The system of claim 3, wherein said client includes a callback mechanism for determining said appropriate authentication mechanism for the server application from among said plurality of the authentication mechanisms.

6. The system of claim 5, wherein said callback mechanism interacts with the subject to determine said appropriate authentication mechanism.

7. The system of claim 5, wherein said callback mechanism accesses a configuration repository to determine said appropriate authentication mechanism.

8. The system of claim 3, wherein said agent includes a mechanism resolver for determining from said plurality of the authentication mechanisms a subset of zero or more of the authentication mechanisms which affects the service provided by the server application.

9. The system of claim 8, wherein said agent further includes an authentication agent for brokering between said client and said mechanism resolver.

10. The system of claim 8, wherein said agent further includes a mechanism repository for storing information about said plurality of the authentication mechanisms and said mechanism resolver queries said mechanism repository when determining said subset of zero or more of the authentication mechanisms which affects the service provided by the server application.

11. The system of claim 10, wherein said agent further includes a mechanism registrator for the authentication mechanism to register in said mechanism repository by adding information about itself.

12. The system of claim 11, wherein said mechanism registrator is further for the authentication mechanism to update itself in said mechanism repository by changing information about itself.

13. The system of claim 4, wherein said protocol proxy resides in said agent domain on the network.

14. The system of claim 1, wherein said protocol proxy resides in the authentication domain on the network.

15. The system of claim 1, wherein said protocol proxy uses a standard security protocol to communicate with said client and a mechanism-specific protocol to communicate with the authentication mechanism.

17. The system of claim 1, wherein at least one of said client and said protocol proxy authenticates using SRP protocol.

18. The system of claim 1, wherein said protocol proxy produces a signed name assertion.

19. The system of claim 18, wherein said signed name assertion is contained in a S2ML document.

20. The system of claim 18, wherein said protocol proxy further produces a signed name entitlement.

21. The system of claim 1, wherein said protocol proxy uses a proxy name assertion to authenticate itself to the client.

22. The system of claim 1, further comprising an adapter for receiving said authentication name assertion, recreating said credentials, and permitting said client to access the server application based on said credentials.

23. A method for authenticating a subject residing in a subject domain on a network to a server application residing in a server domain on the network, wherein an authentication

mechanism residing in an authentication domain on the network affects the service provided by the server application, the method comprising the steps:

(a) authenticating the subject to a protocol proxy with a client by providing subject credentials on behalf of the subject;

(b) obtaining a name assertion from said protocol proxy via the authentication mechanism which will allow said client to access the server application, thereby mediating between said protocol proxy and the authentication mechanism to permit the subject to access the server application via said client;

(c) creating an authentication name assertion with said protocol proxy based on said subject credentials which will allow said client to access the server application;

(d) communicating said authentication name assertion to said client; and

(e) communicating said authentication name assertion to the server application.

24. The method of claim 23, wherein the subject is non-human and said client is integrated into the subject, and the method further comprising:

gathering said subject credentials with said client for the subject; and

communicating said subject credentials to said protocol proxy.

25. The method of claim 23, wherein a plurality of the authentication mechanisms are present on the network, and the method further comprising:

interacting between said client and an agent to chose an appropriate authentication mechanism from among said plurality of the authentication mechanisms, wherein said agent resides in an agent domain on the network.

26. The method of claim 25, further comprising:

interacting between said client and said protocol proxy to determine a specification of the authentication mechanism; and

communicating said specification with said client to said agent.

27. The method of claim 25, further comprising determining an appropriate authentication mechanism for accessing the server application from among said plurality of the authentication mechanisms.

28. The method of claim 27, further comprising interacting with the subject to determine said appropriate authentication mechanism.

29. The method of claim 27, further comprising accessing a configuration repository to determine said appropriate authentication mechanism.

B1

30. The method of claim 27, further comprising:

(f) resolving from said plurality of the authentication mechanisms a subset of zero or more of the authentication mechanisms which affects the service provided by the server application.

31. The method of claim 30, wherein said agent further includes an authentication agent, and the method further comprising:

brokering between and authentication agent and said client in said step (f).

32. The method of claim 30, wherein said agent domain further includes a mechanism repository, and the method further comprising:

storing information about said plurality of the authentication mechanisms in said mechanism repository; and

querying said mechanism repository in said step (f).

33. The method of claim 32, further comprising registering the authentication mechanism in said mechanism repository by adding information about the authentication mechanism.

34. The method of claim 25, wherein said protocol proxy resides in said agent domain on the network.

35. The method of claim 23, wherein said protocol proxy resides in the authentication domain on the network.

36. The method of claim 23, wherein said protocol proxy uses a standard security protocol to communicate with said client and a mechanism-specific protocol to communicate with the authentication mechanism.

37. The method of claim 23, wherein at least one of said client and said protocol proxy authenticates using SRP protocol.

38. The method of claim 23, wherein said protocol proxy produces a signed name assertion.

39. The method of claim 38, wherein said signed name assertion is contained in a S2ML document.

40. The method of claim 38, wherein said protocol proxy further produces a signed name entitlement.

41. The method of claim 23, wherein said protocol proxy uses a proxy name assertion to authenticate itself to the client.

42. The method of claim 23, further comprising an adapter, and the method further comprising:

receiving said authentication name assertion with said adapter;

recreating said credentials with said adapter; and

permitting said client to access the server application based on said credentials.